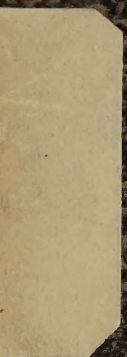


512.73

M57b



THE UNIVERSITY

OF ILLINOIS

LIBRARY

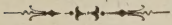
512.813

M57b

MATHEMATICS
DEPARTMENT

Beweis eines von Euler
entdeckten Satzes, betreffend die
Bestimmung von Primzahlen.

INAUGURAL-DISSERTATION
der
mathematischen und naturwissenschaftlichen Facultät
der
KAISER-WILHELMS-UNIVERSITÄT-STRASSBURG
zur
Erlangung der Doktorwürde
vorgelegt von
Peter Meyer
aus Strackholt (Ostfriesland).



STRASSBURG i. E.
Buchdruckerei C. & J. GÖLLER, Magdalenengasse 16.
1906.

5.12.813 ⁷³
M 576

LIBRARY
UNIVERSITY OF ILLINOIS
URBANA

Mit dem Probleme der Ermittlung der Primzahlen haben sich die Mathematiker seit dem Altertum beschäftigt. Es ist seit Euclid bekannt, dass es unendlich viele Primzahlen giebt, da man zu jeder gegebenen Primzahl eine noch grössere bestimmen kann. Aber es ist bis jetzt nicht gelungen, die Gesetzmässigkeit, nach welcher die Primzahlen in der Reihe der ganzen Zahlen verteilt sind, zu bestimmen, noch giebt es eine allgemein gültige Methode, um zu entscheiden, ob eine Zahl Primzahl ist oder nicht. Unter den Mathematikern, die sich mit diesem Problem beschäftigt haben, verdient Fermat an erster Stelle mit genannt zu werden. Fermat hatte die Vermutung ausgesprochen, dass durch die Form $Z = 2^{2^n} + 1$, wenn n die Reihe der ganzen Zahlen durchlaufe, nur Primzahlen ausgedrückt würden. Indes giebt diese Form wohl Primzahlen für $n = 1, 2, 3, 4$; jedoch nicht für $n = 5, 6, 12, 23$. Ebenso werden durch die Form $F = 2^n - 1$, wofern n eine Primzahl ist, in zahlreichen Fällen Primzahlen ausgedrückt. Diese Form hat auch die grösste bis jetzt als Primzahl bewiesene Zahl, nämlich $2^{61} - 1 = 2\,305\,843\,009\,213\,693\,951$. Aber diese Form liefert doch nicht stets unter jener Voraussetzung Primzahlen, denn $2^{11} - 1$ ist z. B. durch 23 teilbar.

Mathematics Research 22 Apr 14 Stecher 35
Se 14 CRAIG LARSEN

264821

Es liegt in der Natur dieser Aufgabe, dass die Schwierigkeit und die Umständlichkeit der Berechnung wächst mit dem Wachstum der Zahlen, welche auf ihren Primzahlcharakter untersucht werden sollen. Für die praktische Berechnung ist es daher von grossem Interesse, solche Methoden zu haben, die auch bei grossen zu untersuchenden Zahlen ohne zu weitläufige Rechnungen zum Ziele führen. Es sei z. B. die Aufgabe gestellt, die Zahl $m = 2^{16} + 1 = 65\,537$ zu untersuchen. Die elementarste Methode besteht darin, dass man die Division von m durch alle Primzahlen $p \leq \sqrt{m}$ versucht, da jede zusammengesetzte Zahl m wenigstens durch eine Primzahl teilbar ist, die kleiner ist als $\sqrt{m}$; ist m durch keine solche Primzahl teilbar, so ist m selbst eine Primzahl.

Eine andere Methode stützt sich auf den Satz: „Jede Primzahl von der Form $4n + 1$ ist stets und nur einmal in die Summe von zwei Quadraten zu zerlegen“. Man hat zu setzen $m = x^2 + y^2$ und kann dann annehmen, dass

$$x^2 \leq y^2, \text{ also } x^2 \leq \frac{m}{2}$$

sei. Man setzt nun Werte für x , die der Bedingung

$$x \leq \sqrt{\frac{m}{2}}$$

genügen, in dem Ausdruck $m - x^2$ ein und untersucht, wie oft dieser Wert eine Quadratzahl wird. Wird der Wert nur einmal zu einem Quadrat, so ist m eine Primzahl. Die Rechnung wird noch wesentlich verkürzt durch Anwendung der Methode der Exklusion¹⁾.

Noch schneller kommt man zum Ziele, wenn man

¹⁾ Vgl. Weber-Wellstein, Encyclopaedie d. Elementarmathematik, Bd. I, p. 251.

eine von Herrn E. Lucas angegebene Methode benutzt ¹⁾, der folgende Umkehrung des Satzes von Fermat zu Grunde liegt:

„Wenn $a^x - 1$ teilbar ist durch n für $x = n - 1$ und nicht teilbar ist für x gleich einem Teiler von $n - 1$, so ist n eine Primzahl“.

Es sei $a = 3$, $n = 65\,537 = 2^{16} + 1$; in diesem Falle sind die Teiler von $n - 1$ sämtlich Potenzen von 2, nämlich: $1\ 2\ 2^2\ 2^3\ \dots\ 2^{16}$. Bildet man die Reste der Division durch n für die Potenzen von 3, wobei zu beachten ist, dass jeder Rest sich aus dem vorhergehenden durch Quadrieren ergibt, so ergeben sich die Reste 3, 9, 81, 6561, $\dots\ 1$. Der Rest 1 ergibt sich erst für $x = n - 1 = 2^{16}$. Also ist $2^{16} + 1$ notwendig eine Primzahl.

Wir sehen an der Betrachtung dieses Beispiels, dass die Prinzipien, welche den Methoden, zu entscheiden, ob eine Zahl Primzahl ist oder nicht, zu Grunde liegen, ganz verschiedener Art sein können. Die zweite Methode beruhte auf dem Satze, dass eine Primzahl von der Form $p = 4n + 1$ stets und nur einmal in die Summe von zwei Quadraten zerlegbar sei; sie führte auf quadratische Formen. Ueberhaupt steht die Theorie der quadratischen Formen in nahem Zusammenhang zu unserm Problem, da die Darstellung von Zahlen eine der Hauptfragen ist, mit denen sich diese Theorie beschäftigt.

Im Zusammenhange mit der Theorie der quadratischen Formen steht auch ein von Euler angegebenes Verfahren zur Bestimmung von Primzahlen ²⁾. Euler hat in einem Briefe aus dem Jahre 1778 folgende von

¹⁾ E. Lucas, *théorie des nombres*, p. 441.

²⁾ *Nouveaux mémoires de l'académie de Berlin*, 1776—78, p. 337.

ihm gemachte Entdeckung mitgeteilt. Er hat eine Anzahl von Zahlen n gefunden, für die der Satz gilt:

„Eine Zahl, die nur einmal in der Form

$$p = x^2 + n y^2$$

darstellbar ist, ist eine Primzahl“.

Es genügen dieser Bedingung 65 Zahlen n und zwar sind es die folgenden:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848.

Euler giebt ein eigenartiges Kennzeichen für die Zahlen n an: Wenn y alle Zahlen durchläuft, für die es $< \sqrt{3m}$ und relativ prim zu n ist, und wenn dann $n + y^2$ entweder eine Primzahl p , oder $2p$ oder p^2 oder 2^k ist, so gehört n zu der Reihe der obigen Zahlen.

Die Zahlen n haben noch eine andere hervorragende Bedeutung: sie sind, als negative Diskriminanten von quadratischen Formen betrachtet, diejenigen Diskriminanten, für die die quadratischen Formen in jedem Geschlechte nur eine Klasse enthalten. Und auf Grund dieses Zusammenhanges mit der Theorie der quadratischen Formen lässt sich auch der Beweis für die Richtigkeit des von Euler entdeckten Satzes erbringen.

Betrachten wir die in dem obigen Satze von Euler angegebenen Darstellungen vom Standpunkte der Theorie der quadratischen Formen, so handelt es sich um die Darstellung von Primzahlen durch Formen $(a, b, c) = (1, 0, n)$.

Nach der Bezeichnung von Gauss sind dies Formen mit der Diskriminante $b^2 - a c = -n$. Bekanntlich werden alle quadratischen Formen von einer bestimmten Diskriminante in Klassen eingeteilt, indem man alle eigentlich äquivalenten Formen derselben Klasse zuteilt, wobei unter eigentlich äquivalenten Formen diejenigen Formen verstanden werden, welche durch eine lineare Substitution

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

mit der Diskriminante $\alpha \delta - \beta \gamma = +1$ in einander übergeführt werden können. Die Anzahl der Klassen von Formen bei gegebener negativer Diskriminante ist endlich, sie fällt zusammen mit der Zahl der reducierten Formen d. h. der Formen, deren Coefficienten der Bedingung genügen: $2 |b| \leq a \leq c$. Ausgenommen sind die beiden einzigen Fälle: $(a, \frac{1}{2} a, c)$ und (a, b, a) . Diese beiden reducierten Formen sind je eigentlich äquivalent mit den ihnen entgegengesetzten, ebenfalls reducierten Formen $(a, -\frac{1}{2} a, c)$ und $(a, -b, a)$. Abgesehen von diesen beiden Ausnahmen lassen sich aber die reducierten Formen als Repräsentanten der Formenklassen betrachten, da in jeder Klasse eine und nur eine reducierte Form vorkommt.

Weiter werden die Klassen der Formen bezüglich einer Diskriminante in Geschlechter eingeteilt ¹⁾. Zu einem Geschlechte vereinigt man diejenigen Klassen von Formen, deren Gesamtcharakter identisch ist, worunter man folgendes versteht: Ist l eine in D , der Diskriminante der Form (a, b, c) aufgehende ungerade Primzahl und m eine durch (a, b, c) darstellbare Zahl, welche relativ prim zu $2 D$ sei — eine Annahme, der

¹⁾ Vgl. Dirichlet-Dedekind, Zahlentheorie, 4. A., S. 313.

stets Genüge geleistet werden kann — so hat für alle solche Zahlen m das Legendre'sche Zeichen

$$\left(\frac{m}{1}\right)$$

eine und dieselbe Bedeutung. Ist ferner $D \equiv 3 \pmod{4}$, $D \equiv 2 \pmod{8}$, $D \equiv 6 \pmod{8}$, $D \equiv 4 \pmod{8}$ und $D \equiv 0 \pmod{8}$, so haben entsprechend die Werte

$$\begin{aligned} & (-1)^{\frac{m-1}{2}}, (-1)^{\frac{1}{8}(m^2-1)}, (-1)^{\frac{1}{2}(m-1) + \frac{1}{8}(m^2-1)}, \\ & (-1)^{\frac{1}{2}(m-1)} \text{ und } (-1)^{\frac{1}{2}(m-1)} \text{ und } (-1)^{\frac{1}{8}(m^2-1)} \end{aligned}$$

dieselbe Bedeutung für alle durch (a, b, c) darstellbaren zu $2D$ relativ primen Zahlen m . Die hier angeführten Zeichen bilden die Charaktere der betreffenden Form, ihre Gesamtheit den Gesamtcharakter der Form.

Da eine Zahl m , die durch eine Form (a, b, c) darstellbar ist, auch durch sämtliche zu ihr eigentlich äquivalenten Formen dargestellt werden kann, so leuchtet unmittelbar ein, dass derselbe Gesamtcharakter allen Formen einer bestimmten Klasse zukommt. Ein Geschlecht umfasst demnach eine bestimmte Zahl von Formenklassen. Ist λ die Anzahl der Charaktere einer Form, so ist, da sämtliche oben angeführten Charaktere den Wert ± 1 annehmen können, die Anzahl aller überhaupt denkbaren Geschlechter 2^λ . Es gilt nun der Satz: „Nur die Hälfte aller denkbaren Geschlechter ist möglich; und diesen möglichen Geschlechtern entsprechen auch wirkliche Geschlechter“. Also ist die Anzahl der Geschlechter gleich $2^{\lambda-1}$; dabei ist λ die Zahl der in D aufgehenden ungeraden Primzahlen für $D \equiv 1 \pmod{4}$, λ ist um 1 grösser in den übrigen Fällen, ausgenommen $D \equiv 0 \pmod{8}$, wo λ um 2 grösser ist. Ist daher die Diskriminante gegeben, so ist die Anzahl der vorhandenen Geschlechter aus ihr unmittelbar zu bestimmen.

Kehren wir nun zu den in unserem Problem gegebenen Formen $(1, 0, n)$ mit der Diskriminante $D = -n$ zurück. Führen wir für diese 65 von Euler angegebenen Zahlen als negative Diskriminanten die Einteilung in Klassen und Geschlechter durch, so genügen diese 65 Zahlen der schon in der Einleitung bemerkten eigentümlichen Bedingung, dass in ihnen die Anzahl der Klassen mit der Anzahl der Geschlechter übereinstimmt, also in jedem Geschlechte nur eine Klasse enthalten ist. Nehmen wir z. B. die Zahl $D = -21$ aus der Reihe jener 65 Zahlen heraus. Die aus der Bedingung $2 \mid b \leq a \leq c$ abgeleiteten, die verschiedenen Klassen repräsentierenden reducierten Formen sind in diesem Falle: $(1, 0, 21)$, $(3, 0, 7)$, $(2, 1, 11)$, $(5, 2, 5)$. Da $D = -21 \equiv 3 \pmod{4}$ ist, so ist die Anzahl der Spezialcharaktere $\lambda = 3$, mithin wird $2^{\lambda-1} = 4$ die Anzahl der Geschlechter. Zu betrachten sind in diesem Falle die Charaktere:

$$\left(-1\right)^{\frac{m-1}{2}}, \left(\frac{m}{3}\right) \text{ und } \left(\frac{m}{7}\right).$$

Eine zu $2D$ relativ prime, durch die reducierten Formen darstellbare Zahl m lässt sich leicht, meistens schon aus den äusseren Coefficienten der Formen bestimmen. Für die Form $(1, 0, 21)$ nehmen wir $m = 1$ aus der Darstellung mit den Unbekannten ($x = 1, y = 0$) dann erhalten die Charaktere folgende Werte:

$$\left(-1\right)^{\frac{m-1}{2}} = +1, \left(\frac{m}{3}\right) = +1, \left(\frac{m}{7}\right) = +1.$$

Der zweiten reducierten Form $(3, 0, 7)$ entspricht, wenn man als darstellbare zu $2D$ relativ prime Zahl aus ($x = 1, y = 2$) die Zahl $m = 31$ nimmt:

$$(-1)^{\frac{m-1}{2}} = -1, \left(\frac{m}{3}\right) = +1, \left(\frac{m}{7}\right) = -1.$$

Der dritten reducierten Form (2, 1, 11) entspricht, wenn man $m = 11$ nimmt aus ($x = 0, y = 1$):

$$(-1)^{\frac{m-1}{2}} = -1, \left(\frac{m}{3}\right) = -1, \left(\frac{m}{7}\right) = +1.$$

Der Form (5, 2, 5) entspricht, wenn man $m = 5$ nimmt aus der Darstellung ($x = 1, y = 0$):

$$(-1)^{\frac{m-1}{2}} = +1, \left(\frac{m}{3}\right) = -1, \left(\frac{m}{7}\right) = -1.$$

Wie man sieht, sind alle diese Geschlechter verschieden d. h. jeder Klasse von Formen entspricht auch ein besonderes Geschlecht; diese Eigentümlichkeit besitzen alle von Euler angegebenen 65 Zahlen.

Die erste nicht zu jenen 65 Zahlen gehörende Diskriminante ist $D = -11$. Da wir später bei der Anwendung auf ein Beispiel auf diese Zahl zurückkommen, so wollen wir auch für $D = -11$ die Klassen und Geschlechter angeben. Es entspricht dieser Diskriminante das Klassensystem: (1, 0, 11), (3, 1, 4), (3, -1, 4). Es ist $D = -11 \equiv 1 \pmod{4}$, also die Zahl der Charaktere $\lambda = 1$, mithin die Zahl der Geschlechter $2^{\lambda-1} = 1$. Nämlich der Form (1, 0, 11) entspricht

$$\left(\frac{1}{11}\right) = +1,$$

der Form (3, 1, 4) entspricht

$$\left(\frac{3}{11}\right) = +1$$

und ebenso entspricht der Form (3, -1, 4) der Wert

$$\left(\frac{3}{11}\right) = +1.$$

Wir gehen jetzt an die Betrachtung unseres Problems selbst. Da die Darstellung von Primzahlen durch bestimmte quadratische Formen das Ziel unserer Untersuchung ist, so haben wir zunächst klarzulegen, wann und wie oft eine bestimmte Zahl m durch eine gegebene quadratische Form darstellbar ist. Damit eine Zahl m durch eine gegebene Form (a, b, c) mit der Diskriminante D darstellbar ist, ist Grundbedingung, dass D quadratischer Rest von m ist, also die Congruenz $x^2 \equiv D \pmod{m}$ Wurzeln hat. Eine solche Congruenz hat, wenn die Anzahl der in m enthaltenen Primfaktoren gleich μ ist und m ungerade ist, 2^μ inkongruente Wurzeln. Es sei n eine bestimmte Wurzel dieser Congruenz, so folgt aus $n^2 \equiv D \pmod{m}$, dass $n^2 - D$ durch m teilbar ist; der Quotient sei l , so ist $n^2 = D + m l$. Dieser Wurzel n entspricht demnach eine Form (m, n, l) mit derselben Diskriminante D . Man untersucht nun, ob die Formen (m, n, l) und (a, b, c) eigentlich äquivalent sind. Dies geschieht durch Ueberführung von (m, n, l) in benachbarte Formen, wodurch man endlich zu einer reducierten Form gelangt, und zwar sind benachbarte Formen im allgemeinen zwei Formen wie (a, b, a') und (a', b', a'') , wenn $b' \equiv -b \pmod{a'}$ und $b + b' = -a' \cdot \delta$ ist; die Substitution, durch die alsdann die erste Form in die zweite übergeführt wird, ist

$$S = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}.$$

Ist (m, n, l) nicht äquivalent mit der reducierten Form (a, b, c) , so ist auch keine zu der Wurzel n gehörige Darstellung von m durch (a, b, c) möglich, ist aber (m, n, l) eigentlich äquivalent der Form (a, b, c) , so

kennt man gleichzeitig durch die Ueberführung von (m, n, l) in benachbarte Formen die Substitution, durch die (m, n, l) in (a, b, c) überzuführen ist. Umgekehrt giebt es dann aber auch eine inverse Substitution

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

durch die (a, b, c) in (m, n, l) übergeht; daraus ergibt sich dann die Darstellung $m = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$.

Weiter ist zu fragen, wie viele Darstellungen von m in diesem Falle zu jeder einzelnen Wurzel n gehören. Die Antwort auf diese Frage giebt uns die Pell'sche Gleichung. Wird nämlich durch die Transformation T die Form (a, b, c) in sich selbst transformiert, so giebt die kombinierte Substitution $T \cdot S$ eine Transformation von (a, b, c) in (m, n, l) ; wenn wir unter S die obige bestimmte Substitution

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

verstehen. Die Frage nach der Anzahl von Transformationen von (a, b, c) in (m, n, l) fällt demnach zusammen mit der Frage nach der Anzahl der Substitutionen T , durch welche (a, b, c) in sich selbst übergeführt wird. Diese Frage ist aber identisch mit der Frage nach der Anzahl der Lösungen der Pell'schen Gleichung: $t^2 - Du^2 = 1$, wo D die Diskriminante von (a, b, c) sei. Ist nämlich (t, u) eine Lösung dieser Gleichung, so giebt die Substitution

$$\begin{pmatrix} \lambda & \mu \\ \nu & \rho \end{pmatrix} = \begin{pmatrix} t - bu & -cu \\ au & t + bu \end{pmatrix}$$

eine Transformation der Form (a, b, c) in sich selbst. Jede kombinierte Substitution

$$S \cdot T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \lambda & \mu \\ \nu & \rho \end{pmatrix}$$

führt (a, b, c) in (m, n, l) über. Nun ist die Anzahl der Lösungen der Pell'schen Gleichung für den Fall $D < 0$ endlich, und zwar ist sie gleich 2 für den Fall $D < -1$, und gleich 4 für den Fall $D = -1$. Für den Fall $D < -1$ haben wir nur die triviale Lösung $t = \pm 1, u = 0$; für $D = -1$ haben wir 4 Lösungen: $t = \pm 1, u = 0$ und $t = 0, u = \pm 1$. Da, wie oben bemerkt, die Anzahl der Wurzeln der Congruenz $x^2 \equiv D \pmod{m}$ gleich 2^μ ist, wenn μ die Anzahl der in m aufgehenden Primfaktoren bei ungeradem m ist, und zu jeder einzelnen Wurzel 2 Darstellungen gehören für $D < 1$, so ist $2 \cdot 2^\mu = 2^{\mu+1}$ die Anzahl der Darstellungen einer Zahl m ; ausgenommen ist der Fall $D = -1$, für den es $4 \cdot 2^\mu = 2^{\mu+2}$ Darstellungen giebt.

Indes reducirt sich die Zahl der Darstellungen, wenn man, wie wir in unserem Probleme, nur nach der Zahl der Zerlegungen einer Zahl in ein Quadrat und in das n fache eines Quadrates fragt. Es entspreche der Wurzel $x = n$ die Substitution

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

von (a, b, c) in (m, n, l) ; dann nennen wir (α, γ) die zur Wurzel n gehörende Darstellung von m . Für $D < -1$ sind die Lösungen der Pell'schen Gleichung

$$t = \pm 1, u = 0;$$

dementsprechend lauten die beiden zur Wurzel $x = n$ gehörenden Substitutionen:

$$S \cdot T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} +1 & 0 \\ 0 & +1 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \text{ und}$$

$$S \cdot T' = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -\alpha & -\beta \\ -\gamma & -\delta \end{pmatrix}.$$

Demnach gehören zu einer bestimmten Wurzel n die

beiden Darstellungen (α, γ) und $(-\alpha, -\gamma)$ von m .
Fragt man sich aber nach der Anzahl der Zerlegungen
von m in ein Quadrat und in das n fache eines Quadrates,
so entspricht jenen beiden Darstellungen eine und die-
selbe Zerlegung.

Ferner, wenn n eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{m}$$

ist, so ist der entgegengesetzte Wert $-n$ auch eine
Wurzel. Wenn die Form (m, n, l) der Wurzel n entsprach,
so entspricht der Wurzel $-n$ die Form $(m, -n, l)$; und
wenn

$$\begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}$$

die durch successive Ueberführung auf benachbarte
Formen entstandene Substitution war, die (m, n, l) in
 (a, b, c) überführte, so wird $(m, -n, l)$ entsprechend
durch die Substitution

$$\begin{pmatrix} 0 & 1 \\ -1 & -\delta \end{pmatrix}$$

in (a, b, c) übergeführt, wie sich unmittelbar durch
Bildung der benachbarten Formen ergibt. Es wird
dann (a, b, c) durch die inverse Substitution

$$\begin{pmatrix} -\delta & -1 \\ +1 & 0 \end{pmatrix}$$

in $(m, -n, l)$ übergeführt oder allgemein ausgedrückt:
wenn (a, b, c) in (m, n, l) überging durch

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

so geht (a, b, c) in $(m, -n, l)$ über durch

$$S' = \begin{pmatrix} -\alpha & \beta \\ +\gamma & \delta \end{pmatrix}.$$

Demnach entsprechen der zu n entgegengesetzten Wurzel $-n$ die beiden Darstellungen $\pm (-\alpha, +\gamma)$ von m durch (a, b, c) . Handelt es sich aber um die Zerlegung in ein Quadrat und in das Vielfache eines Quadrates, so geben diese beiden zuletzt genannten Darstellungen wieder dieselbe Zerlegung wie die zur Wurzel $+n$ gehörenden.

Das Resultat dieser Betrachtungen ist, dass die Zahl der Zerlegungen einer Zahl in ein Quadrat und in das n -fache eines Quadrates sich reduciert auf

$$\frac{1}{4} \cdot 2^{\mu+1} = 2^{\mu-1}$$

aus der Zahl $2^{\mu+1}$ aller möglichen Darstellungen einer Zahl m für $D < -1$. Der Fall $D = -1$, in welchem $2^{\mu+2}$ Darstellungen möglich sind, bildet keine Ausnahme, denn dort kann man, da die einzige reducierte Form $(1, 0, 1)$ symmetrisch bezüglich der äusseren Coefficienten ist, noch die Vertauschung (α, γ) und (γ, α) von Darstellungen vornehmen, so dass in diesem Falle 8 Darstellungen einer Zahl nur eine Zerlegung in Quadrate entspricht. Wir haben somit für die Zerlegungen einer Zahl m keinen Ausnahmefall mehr zu berücksichtigen, sondern ihre Zahl beträgt für negative Diskriminanten in jedem Falle $\nu = 2^{\mu-1}$. Hieraus können wir sogleich entscheiden, wie gross die Zahl der Zerlegungen für eine Primzahl ist. Es wird nämlich für $\mu = 1$ auch der Wert $\nu = 2^{\mu-1} = 1$ d. h. eine Primzahl ist, wenn überhaupt, stets nur einmal in die Form $x^2 + n y^2$ zu zerlegen.

Es ist indes auch der Fall denkbar, dass auch zusammengesetzte Zahlen nur einmal durch $x^2 + n y^2$ darstellbar sind. Um hierfür die Gründe zu finden, haben wir tiefer auf die zahlentheoretischen Eigentüm-

lichkeiten der Zahlen, besonders die Verteilung der sie darstellenden Formen auf Geschlechter einzugehen. Dabei müssen wir nun einen strengen Unterschied machen zwischen denjenigen Diskriminanten, für die alle Formen nur eine Klasse bilden, und denjenigen, für die es mehrere Formenklassen giebt. Einklassig sind die Formen der Diskriminanten -1 , -2 , -3 , -4 , -7 , Bilden wir für sie aus $x^2 \equiv D \pmod{m}$ für die Wurzel n die Form (m, n, l) , so muss diese sicher der einzigen reducierten Form $(a, b, c) = (1, 0, n)$ eigentlich äquivalent sein, da ja hier alle Formen einer Klasse angehören. Mithin giebt es hier auch stets $2^{\mu} - 1$ Zerlegungen einer Zahl m in $(1, 0, n)$, wenn m überhaupt durch eine solche Form darstellbar ist und wenn μ wieder die Zahl der Primfaktoren von m ist. Im Falle, dass m eine Primzahl ist, kann es folglich nur eine Zerlegung von m in $(1, 0, n)$ geben. Die Bedingung aber, dass $m = p$ durch die Form $(1, 0, n)$ überhaupt darstellbar ist, ist, dass

$$\left(\frac{D}{p}\right) = +1$$

wird, wenn D die Diskriminante dieser Form ist. Die Diskriminante -1 , der die einzige reducierte Form $(1, 0, 1)$ entspricht, ist quadratischer Rest für die Primzahlen p von der Form $p = 4n + 1$. Damit haben wir den speziellen Fall, der schon von Euler ¹⁾ bewiesen ist:

„Jede Primzahl von der Form $p = 4n + 1$ ist stets und zwar nur auf eine einzige Art in die Summe zweier Quadrate zu zerlegen“.

Ebenso ist die Diskriminante -2 , der als einzige

¹⁾ Euler, Demonstratio theorematum Fermatiani, omnem numerum . . .

reducierte Form $(1, 0, 2)$ entspricht, quadratischer Rest für alle Primzahlen von der Form $8n + 1$ und $8n + 3$. Hierin liegt der Beweis des zuerst von Lagrange¹⁾ bewiesenen Satzes:

„Jede Primzahl p von der Form $p = 8n + 1$ oder $8n + 3$ lässt sich stets und nur auf eine einzige Weise in die Summe eines Quadrates und des doppelten eines Quadrates zerlegen.“

Die Umkehrung unserer Sätze, welche die Form erhalten würde: „eine Zahl, die nur einmal in der Form $x^2 + ny^2$ darstellbar ist, ist eine Primzahl“ ist damit noch nicht gestattet. Denn eine Zerlegung ergab sich, wenn die Anzahl der verschiedenen in m aufgehenden Primzahlen $\mu = 1$ war. Wir können also nur sagen: eine Zahl, die nur einmal in der Form $x^2 + ny^2$ darstellbar ist, ist eine Primzahl oder Primzahlpotenz. Ist aber eine Primzahlpotenz p^π durch eine primitive Form (a, b, c) darstellbar, d. h. hat die Congruenz $x^2 \equiv D \pmod{p^\pi}$, wo p zum wenigsten in der zweiten Potenz vorkomme, eine Wurzel n , so ist noch um so mehr $x^2 \equiv D \pmod{p}$ für dasselbe $x = n$. Es gehöre zu der Wurzel n die Darstellung

$$p^\pi = a x^2 + 2 b x y + c y^2,$$

so gehört zu derselben Wurzel n auch eine Darstellung

$$p = a x'^2 + 2 b x' y' + c y'^2.$$

In dieser letzten Darstellung sind x' und y' gewiss relativ prim; man nennt eine solche Darstellung eine eigentliche Darstellung. Unter den verschiedenen Darstellungen (x, y) von p^π , welche es geben mag, wird es gewiss auch eine solche geben, in der x^2 und y^2 als grössten gemeinsamen Faktor die gerade in p^π ent-

¹⁾ Lagrange, Recherches d'Arithmétique.

haltene Potenz p^{2^v} von p haben. Denn durch Multiplikation mit p^{2^v} geht die Darstellung

$$p = a x'^2 + 2 b x' y' + c y'^2$$

in eine Darstellung von p^π über. Nun wissen wir aber, dass zu jedem ungeraden in m aufgehenden Primfaktor p^π nur zwei Darstellungen $\pm (x, y)$ gehören. Also müssen in der Darstellung $p^\pi = a x^2 + 2 b x y + c y^2$ die Unbekannten (x, y) den grössten gemeinsamen Teiler p^v haben. Schliessen wir daher diejenigen Darstellungen einer Zahl, in der x und y einen gemeinsamen Teiler haben, von unserer Betrachtung aus, so können wir für unsere oben angegebenen Werte n sagen: eine Zahl, die nur einmal in der Form $x^2 + n y^2$ darstellbar ist, ist eine Primzahl.

Wir haben bislang einklassige Formen $(1, 0, n)$ mit den Diskriminanten $-n = -1, -2, -3, -4, -7$ betrachtet. Umständlicher wird die Behandlung unserer Frage, wenn mehrere Klassen von Formen vorhanden sind, weil hier nicht, wie oben, die durch eine Congruenzwurzel n gebildete Form (m, n, l) notwendig der einen vorhandenen reducierten Form eigentlich äquivalent zu sein braucht.

Hier tritt nun die hervorragende Bedeutung der 65 Euler'schen Zahlen zutage. Es sei m wieder die darzustellende Zahl, von der wir jetzt voraussetzen wollen, dass sie zu $2D$ relativ prim sei, wir dürfen diese Beschränkung machen, weil es uns schliesslich ja auf die Darstellung von Primzahlen ankommt. Die notwendige Bedingung für die Möglichkeit der Darstellung einer Zahl, nämlich dass die Congruenz

$x^2 \equiv D \pmod{m}$ eine Wurzel n haben muss, führt auf die Form $(m, n, 1)$. Jede solche Form $(m, n, 1)$ ist einer und nur einer reducierten Form eigentlich äquivalent, deren Zahl jetzt grösser als 1 vorausgesetzt sei. Im ganzen haben wir wieder, wie vorhin $2^{\mu+1}$ Darstellungen einer Zahl m , die sich aber im allgemeinen auf die sämtlichen reducierten Formen verteilen können, so dass auf eine bestimmte reducierte Form, z. B. auf die Hauptform $(1, 0, -D)$ nicht alle $2^{\mu+1}$ Darstellungen resp. $2^{\mu-1}$ verschiedenen Zerlegungen entfallen. Nur die Formen, die unseren 65 Zahlen als Diskriminanten entsprechen, bilden eine Ausnahme. Sämtliche durch ein Geschlecht von Formen darstellbaren Zahlen m haben einen und denselben Gesamtcharakter. In jenen 65 Fällen entspricht nun aber jedem Geschlechte nur eine Klasse, also auch nur eine einzige reducierte Form. Für eine zu $2D$ relativ prime Zahl m , die hier einmal durch die Hauptform $(1, 0, -D)$ darstellbar ist, können nicht auch einige Darstellungen zu anderen reducierten Formen gehören, weil zwei verschiedenen Formenklassen auch zwei verschiedene Geschlechter entsprechen, und damit die darzustellende Zahl m einmal diesen, das andere Mal einen anderen Gesamtcharakter annehmen müsste, was unmöglich ist. Hierin liegt der Beweis des von Euler ausgesprochenen Satzes: ist die Zahl m , welche μ verschiedene ungerade Primfaktoren habe, einmal durch $(1, 0, -D)$ darstellbar, so entfallen sämtliche möglichen $2^{\mu+1}$ Darstellungen resp. $2^{\mu-1}$ verschiedenen Zerlegungen der Zahl m auf die Form $(1, 0, -D)$. Ist $\mu = 1$, d. h. $m = p$ — wobei der Fall $m = p^2$ gemäss unserer obigen Betrachtung nicht mehr zu beachten ist — so giebt es, wenn p überhaupt in die Form $(1, 0, -D)$ zerlegbar ist, nur eine solche Zerlegung, und umgekehrt gilt für diese

65 Zahlen n und zwar nur für diese der von Euler aufgestellte Satz:

„Eine Zahl, die nur einmal in der Form $x^2 + n y^2$ darstellbar ist, ist eine Primzahl“.

In allen anderen Fällen dagegen ist es möglich, dass sich die Darstellungen einer Zahl m auf verschiedene vorhandene reducierte Formen verteilen, weil dort mehrere Klassen einem Geschlechte angehören. Dort ist es möglich, dass weniger als 2^{u-1} Zerlegungen auf die Hauptform $(1, 0, -D)$ entfallen. Es seien etwa $2^{u-\kappa}$; dann wird in diesem Falle eine Zahl m , die κ verschiedene Primfaktoren enthält, nur einmal in der Form $x^2 + n' y^2$ darstellbar sein.

Zur Erläuterung mögen zwei Beispiele dienen, wobei wir einmal eine Darstellung durch Formen nehmen, deren Diskriminante zu den 65 Euler'schen Zahlen gehört, das andere Mal mag die Diskriminante nicht zu diesen Werten gehören. Wir betrachten zunächst den Fall, wo $D = -12$ sei. Die Formenklassen werden hier repräsentiert durch $(1, 0, 12)$, $(3, 0, 4)$. Ist m die darzustellende Zahl, so muss zunächst die Bedingung

$$\left(\frac{-12}{p}\right) = +1$$

erfüllt sein für jede in der darzustellenden Zahl m enthaltene Primzahl p . Es ist

$$\left(\frac{-12}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right);$$

es ist

$$\left(\frac{p}{3}\right) = +1$$

für alle Primzahlen von der Form $3h + 1$. Wir wollen als ungerade darzustellende Zahl, welche dieser Bedingung genügt, die Zahl $133 = 7 \cdot 19$ wählen. Die

Wurzel der Congruenz $x^2 \equiv -12 \pmod{133}$ sind:
 $n = \pm 11$ und $n' = \pm 46$.

Der Wurzel $+11$ entspricht aus $n^2 + \Delta = m$ eine Form $(m, n, 1) = (133, 11, 1)$. Diese Form haben wir durch successive Ueberführung in benachbarte Formen in eine ihr eigentlich äquivalente reducierte Form überzuführen. Diese Form geht durch die Substitution

$$S = \begin{pmatrix} 0 & 1 \\ -1 & -11 \end{pmatrix}$$

in $(1, 0, 12)$ über; also geht umgekehrt $(1, 0, 12)$ durch die inverse Substitution

$$S = \begin{pmatrix} -11 & -1 \\ +1 & 0 \end{pmatrix}$$

in $(133, 11, 1)$ über. Hieraus folgt eine Darstellung $(-11, +1)$ für 133 durch die Form $(1, 0, 12)$, nämlich $133 = 1 \cdot (-11)^2 + 12 \cdot 1^2$. Die zweite Darstellung, welche der Wurzel $+11$ entspricht, ist die der obigen entgegengesetzte, nämlich $(+11, -1)$. Sie giebt dieselbe Zerlegung von 133. Zu der Wurzel -11 gehören die beiden Darstellungen $\pm(+11, -1)$; diese ergeben auch keine neue Zerlegung in Quadrate.

Die beiden anderen Congruenzwurzeln sind $n' = \pm 46$. Aus $n'^2 + \Delta = m'$ folgt die Form $(133, 46, 16)$. Die Form $(133, 46, 16)$ geht in $(1, 0, 12)$ über durch

$$\begin{pmatrix} -1 & -2 \\ +3 & +5 \end{pmatrix}$$

und umgekehrt geht $(1, 0, 12)$ in $(133, 46, 16)$ über durch die inverse Substitution

$$S = \begin{pmatrix} +5 & +2 \\ -3 & -1 \end{pmatrix}.$$

Diese Substitution ergiebt die Darstellung $(+5, -3)$ von 133 durch die Form $(1, 0, 12)$, nämlich

$$133 = 1 \cdot 5^2 + 12 \cdot (-3)^2.$$

Die zweite zu derselben Wurzel gehörende Darstellung, ebenso die beiden zur Wurzel -46 gehörenden Darstellungen ergeben, wie oben, dieselbe Zerlegung. Man sieht an diesem Beispiele, dass die Darstellungen einer Zahl sich in diesem Falle nicht auf verschiedene reduzierte Formen verteilen, sondern sämtlich einer einzigen angehören, in diesem Falle der Form $(1, 0, 12)$.

Einer zusammengesetzten Zahl entsprechen in diesem Falle auch mehrere Darstellungen.

Nehmen wir dagegen die Primzahl 37 als darzustellende Zahl, so genügt der Congruenz

$$x^2 \equiv -12 \pmod{37}$$

die Wurzel $n = \pm 5$ und nur diese. Aus $n^2 + \Delta = m$ folgt die Form $(m, n, 1) = (37, 5, 1)$, welche durch die Substitution

$$S = \begin{pmatrix} 0 & 1 \\ -1 & -5 \end{pmatrix}$$

in $(1, 0, 12)$ übergeht. Durch die inverse Substitution

$$S' = \begin{pmatrix} -5 & -1 \\ +1 & 0 \end{pmatrix}$$

geht $(1, 0, 12)$ in $(37, 5, 1)$ über. Daraus ergibt sich die Darstellung $(-5, +1)$ von 37 durch die Form $(1, 0, 12)$, nämlich $37 = (-5)^2 + 12 \cdot 1^2$. Die andere zu $n = +5$ gehörende Darstellung, sowie die beiden zu $n = -5$ gehörenden Darstellungen ergeben dieselbe Zerlegung von 37.

Im Gegensatz zu wollen wir nun auch die Darstellung einer Zahl betrachten für den Fall, dass die Diskriminante nicht zu den 65 Zahlen Eulers gehört. In der Reihe der natürlichen Zahlen ist die erste solche Zahl die Zahl 11. Betrachten wir nun die Darstellung

von Zahlen durch quadratische Formen mit der Diskriminante $D = -11$. Ist m die darzustellende Zahl so muss für jede in m aufgehende Primzahl

$$\left(\frac{-11}{p}\right) = +1$$

sein. Es ist

$$\left(\frac{-11}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{11}{p}\right) = \left(\frac{p}{11}\right),$$

es wird

$$\left(\frac{p}{11}\right) = +1$$

für die Primzahlen von der Form

$$p = 11n + 1, 11n + 3, 11n + 4, 11n + 5,$$

wie sich mittelst der Theorie der quadratischen Reste bestimmen lässt¹⁾. Die darzustellende Zahl m darf also nur Primfaktoren von dieser Gestalt enthalten. Eine solche Zahl ist $m = 3 \cdot 5 = 15$. Im ganzen giebt es $2^{\mu+1} = 8$ Darstellungen von $m = 15$, zu jeder der 4 Wurzeln gehören zwei. Die 4 Congruenzwurzeln der Congruenz $x^2 \equiv -11 \pmod{15}$ sind:

$$n = \pm 2, n = \pm 7.$$

Der Wurzel $n = +2$ entspricht aus $n^2 + \Delta = m$ die Form $(m, n, 1) = (15, 2, 1)$.

Die reducierten Formen bezüglich der Diskriminanten $D = -11$ sind:

$$(1, 0, 11), (3, +1, 4), (3, -1, 4).$$

Wir haben nun zu untersuchen, welcher der reducierten Formen die Form $(15, 2, 1)$ eigentlich äquivalent ist. Es geht $(15, 2, 1)$ durch die Substitution

¹⁾ vergl. Dirichlet-Dedekind, Zahlentheorie, S. 98.

$$\begin{pmatrix} 0 & 1 \\ -1 & -2 \end{pmatrix}$$

über in die Form (1, 0, 11). Umgekehrt geht durch die inverse Substitution

$$\begin{pmatrix} -2 & -1 \\ +1 & 0 \end{pmatrix}$$

die Form (1, 0, 11) in (15, 2, 1) über. Daraus ergibt sich die Darstellung $(-2, +1)$ für die Zahl 15, nämlich $15 = 1 \cdot (-2)^2 + 11 \cdot 1^2$. Die andere zur Wurzel $+2$ gehörende Darstellung, sowie die beiden zur Wurzel -2 gehörenden, ergeben wieder dieselbe Zerlegung.

Betrachten wir die Wurzel $n = +7$, so wird jetzt $(m, n, 1) = (15, 7, 4)$; es ist zu fragen, zu welcher reduzierten Form diese Form eigentlich äquivalent ist. Es geht (15, 7, 4) über in (3, -1 , 4) durch die Substitution

$$S = \begin{pmatrix} -1 & 0 \\ +2 & -1 \end{pmatrix}$$

und umgekehrt geht (3, -1 , 4) über in (15, 7, 4) durch

$$S' = \begin{pmatrix} -1 & 0 \\ -2 & -1 \end{pmatrix}.$$

Daraus ergibt sich als Darstellung der Zahl 15 durch die Form (3, -1 , 4) die folgende:

$$15 = 3 \cdot (-1)^2 - 2 \cdot 1 \cdot 2 + 4 \cdot (-2)^2.$$

Die andere zur Wurzel $+7$ gehörende Darstellung von 15 unterscheidet sich von dieser nur durch die Vorzeichen der darzustellenden Zahlen.

Die der Wurzel -7 entsprechende Form (15, -7 , 4) ist äquivalent der Form (3, $+1$, 4); analog zu obigem ergibt sich die Darstellung $\pm (-1, +2)$ von 15 durch die reduzierte Form (3, $+1$, 4).

Wir sehen sofort den Unterschied zwischen diesem und dem vorhergehenden Beispiel. Die Darstellungen von m gehören hier nicht alle derselben reducierten Form an; in diesem Falle verteilten sich die Darstellungen auf alle drei reducierten Formen. Dies ist möglich, weil, wie wir früher gezeigt haben, hier alle Klassen einem Geschlechte angehören. Auf die Hauptform $(1, 0, 11)$ entfiel dieses Mal nur eine Zerlegung von $m = 15$; mithin haben wir hier einen Fall, dass eine Zahl nur einmal in der Form $x^2 + ny^2$ darstellbar ist und doch keine Primzahl, sondern zusammengesetzt ist.

Unser Beweis führt uns aber noch über die von Euler aufgestellte Behauptung hinaus. In der Form, wie Euler den Satz ausgesprochen hat, wird das Hauptgeschlecht und die Hauptform $(1, 0, n)$ vor den übrigen reducierten Formen bevorzugt. Hierzu ist aber kein Grund vorhanden. Was für die Hauptform gilt, gilt in diesen 65 Fällen auch für die übrigen reducierten Formen, nämlich, wenn eine Zahl m einmal durch eine bestimmte reducierte Form ausdrückbar ist, so finden ihre sämtlichen Darstellungen durch diese reducierte Form statt. Erforderlich ist nur, dass die durch den Wechsel der Vorzeichen aus einer bestimmten Darstellung $(+x, +y)$ entstehenden Darstellungen keine neue Darstellung der betreffenden Zahl ergeben, dann beträgt die Zahl der von einander verschiedenen Darstellungen einer Zahl stets 2^{u-1} , und hieraus folgt der Satz Eulers. Diese Bedingung erfüllen aber diejenigen reducierten Formen, in denen der mittlere Coefficient $b = 0$ ist, Formen, die zu den ambiguen Formen gehören und bei denen es sich stets um eine Zerlegung einer Zahl in Vielfache von Quadraten handelt. Ist allgemein $(a, 0, c)$ eine solche reducierte Form und gehört ihre Diskrimi-

nante — $a c = D$ zu den 65 Zahlen Eulers, so gilt allgemein der Satz:

„Eine Zahl, die nur einmal in der Form $(a, 0, c)$ darstellbar ist, ist eine Primzahl“.

Damit erscheint der Satz von Euler als Spezialfall eines viel umfassenderen Satzes. Diese Verallgemeinerung des Satzes von Euler hat P. Seelhoff verwertet und zur Bestimmung grosser Primzahlen benutzt ¹⁾. Wir haben in unserem Beweise nur nachgewiesen, dass für die 65 Zahlen Eulers notwendig sämtliche Darstellungen einer Zahl auf eine einzige reducierte Form entfallen müssen. Seelhoff hat noch eine grössere Zahl von Diskriminanten — im ganzen 170 — gefunden, für welche diese Relation besteht. Einer ähnlichen Erweiterung des Satzes von Euler hat sich Pepin ²⁾ bedient, der auch diejenigen Diskriminanten, für die in jedem Geschlechte nur drei Klassen vorhanden sind, zur Bestimmung von Primzahlen benutzt.

Zum Schlusse müssen wir noch auf eine Unbestimmtheit aufmerksam machen, der der Satz von Euler unterliegt. Die Behauptung, dass nur die obigen 65 Zahlen n notwendig jener Beziehung genügen, ist nur insofern richtig, als sich beweisen lässt, dass über —1848 hinaus es keine negative Diskriminante mehr giebt, für die in jedem Geschlechte nur eine Klasse enthalten ist.

¹⁾ P. Seelhoff, Prüfung grösserer Zahlen auf ihre Eigenschaft als Primzahlen. American Journal of Mathematics, Vol. VII, p. 264.

²⁾ Pepin, Extension de la méthode d'Euler . . . Atti dell' Accademia Pontificia, Vol. IX, p. 47, 1893.

Dieser Beweis ist aber bislang nicht gebracht worden. Es haben sich im Allgemeinen nur Annäherungswerte für die Zahl der Klassen und ihre Verteilung in Geschlechtern angeben lassen ¹⁾.

Das Aufhören der einklassigen Formen von einer bestimmten negativen Diskriminante ab steht augenscheinlich in Zusammenhang mit der Verteilung der Primzahlen in der Reihe der ganzen Zahlen. Wir wollen uns, um dies zu zeigen, der seit Kronecker wieder gebräuchlichen und in mancher Hinsicht zweckmässigeren Bezeichnung der quadratischen Formen bedienen, nämlich

$$\varphi = ax^2 + bxy + cy^2 \text{ und } D = b^2 - 4ac$$

die Diskriminante dieser Form nennen. Nach dieser Bezeichnung sind die Formen von den Diskriminanten

$$-3, -4, -7, -11, -19, -43, -67, -163$$

einklassig. Man bestimmt auch hier die Klassenzahl durch Bildung der reduzierten Formen, die hier der Bedingung $|b| \leq a \leq c$ genügen müssen. Daraus folgt, dass b nur die Werte annehmen kann, für die

$$|b| \leq \sqrt{\frac{\Delta}{3}}$$

ist; ferner ist $b \equiv \Delta \pmod{2}$. Die äusseren Coefficienten a und c der reduzierten Form bestimmt man aus

$$\frac{\Delta + b^2}{4} = a \cdot c.$$

Man erhält nun stets nur eine reduzierte Form, wenn die Reihe der Werte

$$\frac{\Delta + b^2}{4}$$

aus lauter Primzahlen besteht, denn dann lassen sie

¹⁾ Gauss, Disqu. arithm. art. 301, 302.

alle nur die eine Zerlegung 1 . p zu. In diesem Falle ist sodann nur die eine Form, die dem Werte $b = \pm 1$ entspricht, reduciert, weil bei allen grösseren Werten von b nicht mehr die Relation $|b| \leq a \leq c$ besteht.

Wir wollen dies an den beiden grössten von den obigen negativen Diskriminanten erläutern. Für

$$D = -67 \text{ ist } |b| \leq \sqrt{\frac{\Delta}{3}} : \pm 1, \pm 3.$$

Dementsprechend erhält man für

$$\frac{\Delta + b^2}{4} = ac : 17, 19,$$

die einzigen Zerlegungen von ac sind: 1.17 und 1.19; als einzige reducierte Form für diese Diskriminante ergibt sich $(1, \pm 1, 17)$.

Für $D = -163$ kann $|b|$ folgende Werte annehmen: $\pm 1, \pm 3, \pm 5, \pm 7$.

Ihnen entsprechen für a . c die Ausdrücke:

$$41, 43, 47, 53.$$

Die einzige reducierte Form für $D = -163$ ist $(1, \pm 1, 41)$.

Die Reihe der Werte

$$\frac{\Delta + b^2}{4} = ac$$

wird nach einem unmittelbar zu übersehenden Gesetze gebildet. Jedesmal, wenn die so gebildete Reihe von Zahlen aus lauter Primzahlen besteht, erhalten wir bestimmt eine Diskriminante, für welche die Formen nur eine Klasse bilden. Diese Verteilung von Primzahlen ist also hierfür eine hinreichende Bedingung. Dass sie unbedingt notwendig ist, lässt sich jedoch nicht beweisen; es wäre nämlich denkbar, dass in einer nach

dem obigen Gesetze gebildeten Reihe von Zahlen auch eine zusammengesetzte Zahl vorkäme, diese aber nur so zu zerlegen wäre, dass die jener Zerlegung entsprechende Form keine reducierte Form würde. Tatsächlich giebt es über die Zahlenreihe: 41, 43, 47, 53 hinaus keine nach demselben Gesetze gebildete Reihe mehr, welche aus lauter Primzahlen besteht, und über die ihnen entsprechende Diskriminante — 163 hinaus hat man keine negative Diskriminante gefunden, der nur eine Klasse von Formen entspricht.

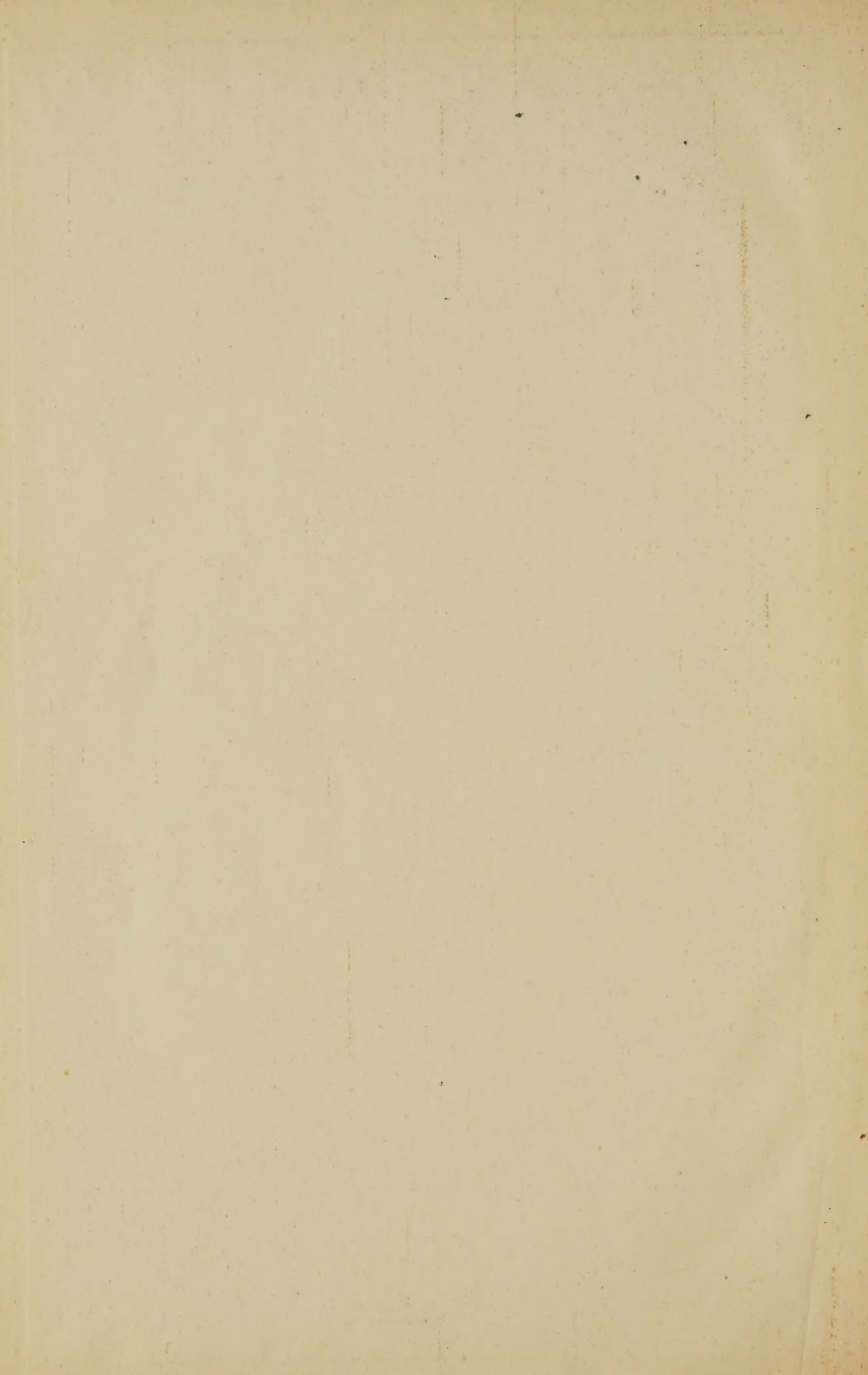
Vita.



Ich, Peter Gerdes Meyer, wurde am 7. Februar 1882 als Sohn des Landwirts Johann J. Meyer zu Strackholt (Ostfriesland) geboren. Bis zu meinem 14. Lebensjahre besuchte ich die Volksschule zu Strackholt und trat dann, durch Privatunterricht vorbereitet, Michaelis 1895 in die Quarta des Gymnasiums zu Aurich ein, welches ich Ostern 1902 mit dem Zeugnis der Reife verliess. Ich widmete mich dem Studium der Mathematik, Physik und Geographie zuerst in Strassburg, dann in Berlin und seit dem Wintersemester 1904 wieder in Strassburg.

Allen meinen Lehrern spreche ich an dieser Stelle meinen besten Dank aus; besonders gilt dieser Dank Herrn Professor Dr. Weber, der mir die Anregung zu vorliegender Arbeit gegeben hat.





UNIVERSITY OF ILLINOIS-URBANA

512.73M57B

C001

BEWEIS EINES VON EULER ENTDECKTEN SATZES



3 0112 017075364